

Self-dual Permutation Codes of Finite Groups in Semisimple Case *

Yun Fan, Guanghui Zhang

Department of Mathematics, Central China Normal University
Wuhan, 430079, China
Email: yunfan02@yahoo.com.cn

Abstract

The existence and construction of self-dual codes in a permutation module of a finite group for the semisimple case are described from two aspects, one is from the point of view of the composition factors which are self-dual modules, the other one is from the point of view of the Galois group of the coefficient field.

Key words. Finite group, permutation code, self-dual module, self-dual code.

1 Introduction

Let F be a finite field of order q which is a power of a prime integer; and let X be a finite set. By FX we denote the F -vector space with the basis X and with the usual scalar product as its standard inner product. Any subspace C of FX is just the usual linear code over F . In coding-theoretic notation, with respect to the standard inner product, the orthogonal subspace C^\perp of a linear code C is called the *dual code* of C ; and C is called a *self-orthogonal code* if $C \subseteq C^\perp$; and C is called a *self-dual code* if $C = C^\perp$.

If X is a group, then FX is an algebra with multiplication induced by the multiplication of the group X , which is called the group algebra of the group X over F ; and any left ideal C of FX is said to be a *group code*. It is an interesting question to find conditions such that a group algebra has a self-dual group codes. More generally, this question can be extended to the group algebras over finite rings.

In [9], finite abelian groups are considered and some results on the non-existence of self-dual group codes are shown. For the direct product of a finite 2-group and a finite $2'$ -group, reference [4] showed when the self-dual group codes do not exist. Using the representation theory of finite groups, for group algebras over finite Galois rings reference [11] gave a complete answer for this

*Supported by NSFC Grant No. 10871079.

question. In particular, it is an easy conclusion that there is no self-dual code for finite groups of odd order.

Thus it is reasonable to consider the self-dual extended group codes for finite groups of odd order. And [7] obtained some interesting conditions for the existence of such self-dual codes in characteristic 2: one is from the point of view of self-dual modules, another one is an elementary number-theoretical condition; and [7] also showed some constructions of such codes.

Extending group codes, [3] discussed the so-called *permutation codes* of finite groups. If G is a finite group and X is a finite G -set, then FX is called a *permutation FG -module*, which has the standard inner product with respect to the basis X ; any FG -submodule C of FX is said to be an *FG -permutation code*. If X is a transitive G -set, the permutation codes of FX is called *transitive permutation codes*. View the base set of the group G as a left regular G -set, then the group codes are just the permutation codes of FG . Some important codes are permutation codes in natural ways, but may not be group codes; e.g. the so-called *multiple-cyclic codes*; see [3] for details. Moreover, the research of permutation codes is of interests from the point of view of automorphism groups of linear codes, for: any permutation automorphism of a linear code is just a permutation of the standard basis of the linear code. In [3] some conditions are obtained for the non-existence of the self-dual transitive permutation codes of finite groups. And it is also an easy conclusion that there is no self-dual transitive permutation code for finite groups of odd order.

In this paper we discuss the existence and construction of self-dual permutation codes for the semisimple case. The outline is as follows.

Throughout the paper, F denotes a finite field of order q , and G denotes a finite group of order coprime to q , and any FG -module is finite-dimensional.

In §2, we first make observations on the related module-theoretical aspects, and then turn to the permutation codes. Since FG is a semisimple algebra (Maschke's theorem), any FG -module V is decomposed into a direct sum of irreducible FG -modules with the collection of the irreducible summands is unique determined up to isomorphism; any irreducible FG -module W which appears in the direct sum is called a *composition factor* of V , and the number of the direct summands which are isomorphic to W is called the *multiplicity* of W in V . The dual space $V^* := \text{Hom}_F(V, F)$ consisting of all the linear form of V is an FG -module with G -action: $(g\varphi)(v) = \varphi(g^{-1}v)$, $\forall g \in G, \varphi \in \text{Hom}_F(V, F), v \in V$. We call V a *self-dual FG -module* if $V \cong V^*$. So, “self-dual module” and “self-dual code” are different concepts. After the module-theoretical results which we need are obtained, we turn to coding-theoretical notation, and show that, for even q and odd $|G|$, an FG -permutation module FX has self-dual permutation codes if and only if any self-dual composition factor of the FG -module FX has even multiplicity. For odd q , only a sufficient condition is obtained.

In §3, we discuss transitive permutation codes, i.e. codes of an permutation module FX with a transitive G -set X . We first reduce the existence of the so-called self-dual *extended transitive permutation codes* to the existence of such transitive permutation codes C of FX that $C^\perp = C \oplus F$. And we show that, for a transitive G -set X with length $n = |X|$, if the integer q as an element of the multiplicative group \mathbb{Z}_n^\times has odd order, then there is a permutation code C of FX such that $C^\perp = C \oplus F$. It is easy to see that this elementary number-theoretical condition is similar to that in [7]. However, the situation of transitive

permutation codes is more delicate than that of group codes, so that we take a way different from [7] to treat our cases; and we obtained no necessary and sufficient conditions, though some more results are shown in §3 which seem interesting.

2 Self-dual modules and self-dual codes

We adopt the usual notation about linear forms, bilinear forms etc. from the usual linear algebra. A bilinear form $f(-, -)$ on an FG -module V is said to be G -invariant if

$$f(g(u), g(v)) = f(u, v), \quad \forall u, v \in V.$$

Let V be an FG -module with a G -invariant non-degenerate bilinear form $\langle -, - \rangle$. Let U, W be submodules of V . Denote

$$\text{Ann}_W^l(U) = \{w \in W \mid \langle w, u \rangle = 0, \forall u \in U\},$$

$$\text{Ann}_W^r(U) = \{w \in W \mid \langle u, w \rangle = 0, \forall u \in U\};$$

in particular, denote $U^\perp = \text{Ann}_V^r(U)$ and ${}^\perp U = \text{Ann}_V^l(U)$. From the G -invariance of $\langle -, - \rangle$, it is easy to see that $\text{Ann}_W^l(U)$ and $\text{Ann}_W^r(U)$ are FG -submodules. Note that $\text{Ann}_W^l(U) = \text{Ann}_W^r(U)$ and ${}^\perp U = U^\perp$ once $\langle -, - \rangle$ is symmetric. For any $v_0 \in V$ we have the linear form $\langle -, v_0 \rangle : V \rightarrow F, v \mapsto \langle v, v_0 \rangle$; and restricting it to U , we have the linear form $\langle -, v_0 \rangle|_U$ on U and it is easy to check that

$$V \longrightarrow U^*, \quad v_0 \longmapsto \langle -, v_0 \rangle|_U \quad (1)$$

is a surjective FG -homomorphism with kernel U^\perp ; thus we have an exact sequence of FG -homomorphisms:

$$0 \longrightarrow U^\perp \longrightarrow V \longrightarrow U^* \longrightarrow 0; \quad (2)$$

in particular, $\dim V = \dim U + \dim U^\perp$ because $\dim U = \dim U^*$. Restricting the bilinear form $\langle -, - \rangle$ to the FG -submodule U , we get a G -invariant symmetric bilinear form on U . If the restricted bilinear form on U is non-degenerate (equivalently, $\text{Ann}_U^r(U) = U \cap U^\perp = 0$), we say that U is a *non-degenerate submodule*. On the other hand, if the restricted bilinear form on U is zero (equivalently, $U \subseteq U^\perp$), we say, in module-theoretical notation, that U is an *isotropic submodule*.

Recall that any FG -module V is written into a direct sum of irreducible modules, and the irreducible direct summands are partitioned by isomorphism, hence $V = V_1 \oplus \cdots \oplus V_h$, with every V_i consisting of the irreducible direct summands which are isomorphic to one and the same irreducible module W_i , but V_i and V_j for $i \neq j$ have no composition factors in common; thus $V_i \cong m_i W_i$ with m_i being the multiplicity of W_i in V , and V_i is called the *homogeneous component* of V associated with the irreducible module W_i , and $V = V_1 \oplus \cdots \oplus V_h$ is called the *canonical decomposition* (or *homogeneous decomposition*) of V , see [10, §2.6]; the canonical decomposition of V is unique, so that for any submodule U of V we have

$$U = (U \cap V_1) \oplus \cdots \oplus (U \cap V_h). \quad (3)$$

Lemma 1. *Let V be an FG -module with a G -invariant non-degenerate bilinear form; and U be an FG -submodule.*

- (1) *If U is non-degenerate then U is a self-dual FG -module.*
- (2) *If U is irreducible, then U is either non-degenerate or isotropic.*
- (3) *If U is a homogeneous component associated with an irreducible module W , then W is self-dual if and only if U is non-degenerate. W is not self-dual if and only if U is isotropic.*

Proof. (1). The non-degeneracy of U implies $U \cap U^\perp = 0$; thus from that $\dim V = \dim U + \dim U^\perp$ we get $V = U^\perp \oplus U$, and it follows from the exact sequence (2) that $U \cong V/U^\perp \cong U^*$.

(2). Because $U \cap U^\perp$ is an FG -submodule of U , the irreducibility of U implies that either $U \cap U^\perp = 0$ or $U \cap U^\perp = U$.

(3). From the exact sequence (2) and the semi-simplicity, we have that $V = U^\perp \oplus U'$ with $U' \cong U^*$. Since FG is an Frobenius algebra, it is known (e.g. see [12]) that the dual modules of all the composition factors of U are just all the composition factors of U^* . Thus U' is a homogeneous component too. Thus the conclusions follows from the uniqueness of the homogeneous decomposition.

Remark. It is well-known that “there is a G -invariant non-degenerate bilinear form on a FG -module V if and only if V is a self-dual FG -module”. The necessity is a special case of Lemma 1(1); and the sufficiency follows that, with an FG -isomorphism $\alpha : V \rightarrow V^*$, the composition map

$$\begin{array}{ccccc} V \times V & \longrightarrow & V^* \times V & \longrightarrow & F, \\ (v, v') & \longmapsto & (\alpha(v), v') & \longmapsto & \alpha(v)(v'). \end{array}$$

is a G -invariant non-degenerate bilinear form on V . For more details, please see [6, Ch.VII, §8].

Lemma 2. *Let V be an FG -module with a G -invariant non-degenerate symmetric bilinear form; let U be an isotropic FG -submodule of V . Then the following are equivalent:*

- (i) $U^\perp = U$;
- (ii) $\dim U = \dim V/2$;
- (iii) *the collection of the composition factors of U and the dual modules of the composition factors of U is the collection of the composition factors of V .*

Proof. (i) \Leftrightarrow (ii) is obvious since $\dim V = \dim U^\perp + \dim U$.

(i) \Leftrightarrow (iii). Similar to the proof for Lemma 1(3), $V = U^\perp \oplus U'$ with $U' \cong U^*$; but now $U \subseteq U^\perp$ by hypothesis, so the equivalence is obvious.

Recall from the usual linear algebra that, for an FG -module V , any bilinear form f on V corresponds to exactly one linear form \bar{f} on the tensor product space $V \otimes_F V$: $\bar{f}(v \otimes v') = f(v, v')$; in other words, the dual space $(V \otimes_F V)^*$ is identified with the space of all the bilinear forms on V . As usually, $V \otimes_F V$ is an FG -module by diagonal action of G , hence $(V \otimes_F V)^*$ is also an FG -module by diagonal action of G ; and the space of all the G -invariant bilinear forms is identified with the subspace of all the G -fixed points of $(V \otimes_F V)^*$, denoted by $((V \otimes_F V)^*)^G$.

On the other hand, G acts on the space $\text{Hom}_F(V, V)$ of all the linear transformations of V in the following way:

$$(g\alpha)(v) = g(\alpha(g^{-1}v)), \quad \forall g \in G, \alpha \in \text{Hom}(V, V), v \in V;$$

and the subspace $\text{Hom}_{FG}(V, V)$ of all the FG -endomorphisms of V is just the set of all the G -fixed points of $\text{Hom}_F(V, V)$.

Lemma 3. *Let V be an FG -module with a G -invariant non-degenerate symmetric bilinear form $\langle -, - \rangle$. For any linear transformation $\alpha \in \text{Hom}_F(V, V)$ define*

$$\varphi_\alpha(u, v) = \langle \alpha(u), v \rangle, \quad \forall u, v \in V.$$

Then φ_α is a bilinear form on V , and

$$\varphi : \text{Hom}_F(V, V) \longrightarrow (V \otimes_F V)^*, \quad \alpha \longmapsto \varphi_\alpha.$$

is an FG -isomorphism, and:

- (1) φ_α is G -invariant if and only if α is an FG -endomorphism;
- (2) φ_α is non-degenerate if and only if α is a non-degenerate transformation;
- (3) φ_α is a symmetric if and only if α is a symmetric transformation.

Proof. It is easy to check that φ_α is a bilinear form on V , and that φ is a linear map; and that φ is injective because $\langle -, - \rangle$ is non-degenerate, hence φ is bijective since $\dim \text{Hom}_F(V, V) = \dim(V \otimes_F V)^*$. Next, for any $g \in G$, any $\alpha \in \text{Hom}_F(V, V)$, and any $u, v \in V$, we have

$$\begin{aligned} \varphi_{g\alpha}(u \otimes v) &= \langle (g\alpha)(u), v \rangle = \langle g\alpha(g^{-1}u), v \rangle = \langle \alpha(g^{-1}u), g^{-1}v \rangle \\ &= \varphi_\alpha(g^{-1}u \otimes g^{-1}v) = \varphi_\alpha(g^{-1}(u \otimes v)) = (g\varphi_\alpha)(u \otimes v). \end{aligned}$$

So φ is an FG -isomorphism. Hence we have the following isomorphism

$$\text{Hom}_{FG}(V, V) \xrightarrow{\cong} ((V \otimes_F V)^*)^G, \quad \alpha \longmapsto \varphi_\alpha; \quad (4)$$

that is, (1) holds. The (2) and (3) can be verified straightforwardly.

Let V and V' be FG -modules equipped with G -invariant bilinear forms f and f' respectively. We say that an FG -homomorphism $\alpha : V \rightarrow V'$ is compatible with the bilinear forms f and f' if $f'(\alpha(u), \alpha(v)) = f(u, v)$ for all $u, v \in V$.

If f is a non-degenerate bilinear form on V , then any FG -homomorphism $\alpha : V \rightarrow V'$ which is compatible with f and f' must be injective; for: $\alpha(u) = 0$ implies that for any $v \in V$ we have that $f(u, v) = f'(\alpha(u), \alpha(v)) = f'(0, \alpha(v)) = 0$, hence $u = 0$ by the non-degeneracy of the form f .

Lemma 4. *Assume that q is even, and V is a self-dual irreducible FG -module. If both f and f' are G -invariant non-degenerate symmetric bilinear forms on V , then there is an FG -automorphism $\beta : V \rightarrow V$ which is compatible with f and f' .*

Proof. Apply the isomorphism (4) to the FG -module V with the G -invariant non-degenerate symmetric bilinear form f . Since V is irreducible, by the Schur's lemma, $\tilde{F} := \text{Hom}_{FG}(V, V)$ is a finite dimensional division F -algebra, hence \tilde{F} is a field extension of F as it is finite. By the commutativity

of \tilde{F} , it is easy to check that the sum and the product of any two symmetric transformations in \tilde{F} are still symmetric transformations, so all the symmetric transformations in \tilde{F} form a subfield \hat{F} of \tilde{F} .

By Lemma 3, for the G -invariant non-degenerate symmetric bilinear form f' , there is an $\alpha \in \hat{F} - \{0\}$ such that

$$f'(u, v) = \varphi_\alpha(u, v) = f(\alpha(u), v), \quad \forall u, v \in V.$$

Since \hat{F} is a finite field of characteristic 2, the map $\hat{F} \rightarrow \hat{F}$, $\lambda \mapsto \lambda^2$, is an automorphism of \hat{F} . So there is a $\beta \in \hat{F}$ such that $\beta^2 = \alpha^{-1}$. Then $\beta : V \rightarrow V$ is an FG -automorphism of V and a symmetric transformation with respect to the bilinear form f ; and, noting that $\alpha\beta = \beta\alpha$, for any $u, v \in V$ we have

$$f'(\beta(u), \beta(v)) = f(\alpha(\beta(u)), \beta(v)) = f((\beta\alpha\beta)(u), v) = f(u, v).$$

That is, β is compatible with the bilinear form f and f' .

Theorem 1. *Let F be a finite field of characteristic 2 and G be a finite group of odd order. Let V be an FG -module with a G -invariant non-degenerate symmetric bilinear form. Then the following are equivalent:*

- (i) *every self-dual composition factor of V has even multiplicity;*
- (ii) *there is an FG -submodule U of V such that $U^\perp = U$.*

Proof. We denote $\langle -, - \rangle$ for the G -invariant non-degenerate symmetric bilinear form on V .

(ii) \Rightarrow (i). This is an easy consequence of Lemma 2 (i) \Rightarrow (iii).

(i) \Rightarrow (ii). Let W be an irreducible FG -submodule of V .

Case 1: $W \subseteq W^\perp$. By the exact sequence (2), we have a submodule W' of V such that $V = W^\perp \oplus W'$ and the homomorphism (1) induces an isomorphism

$$W' \xrightarrow{\cong} W^*, \quad w' \mapsto \langle w', - \rangle|_W.$$

Therefore, the matrix of the symmetric bilinear form $\langle -, - \rangle|_{W' \oplus W}$ restricted to $W' \oplus W$ is as follows

$$\begin{pmatrix} 0 & A \\ A^T & * \end{pmatrix}$$

where A is the matrix of the bilinear form $W' \times W \rightarrow F$, $(w', w) \mapsto \langle w', w \rangle$ and A^T denotes the transpose of A ; so A is invertible, and hence $W' \oplus W$ is a non-degenerate submodule of V . Then

$$V = (W' \oplus W) \oplus (W' \oplus W)^\perp$$

and $(W' \oplus W)^\perp$ is also non-degenerate submodule.

If W is not a self-dual module, then $W' \cong W^*$ is not self-dual, and hence $(W' \oplus W)^\perp$ also satisfies the condition (i). Otherwise, W is a self-dual module, and $W' \cong W^* \cong W$ is a self-dual module too, hence $(W' \oplus W)^\perp$ still satisfies the condition (i). In a word, by induction, there is a submodule S of $(W' \oplus W)^\perp$ such that $\text{Ann}_{(W' \oplus W)^\perp}(S) = S$. Take $U = W \oplus S$; then it is easy to check that $U^\perp = U$ and (ii) holds.

Case 2: $W \not\subseteq W^\perp$. Then W is non-degenerate, i.e. $V = W \oplus W^\perp$, and W is a self-dual module, see Lemma 1(2). By the condition (i), there is a direct decomposition $W^\perp = \tilde{W} \oplus U$ such that $\tilde{W} \cong W$, and $V = W \oplus \tilde{W} \oplus U$.

If $\tilde{W} \subseteq \tilde{W}^\perp$, then it is reduced to Case 1 and the (ii) holds by induction. So we assume that $\tilde{W} \not\subseteq \tilde{W}^\perp$, and hence \tilde{W} is also non-degenerate. Since $W \perp \tilde{W}$, the submodule $W \oplus \tilde{W}$ is non-degenerate too.

Let f and \tilde{f} denote the restrictions of $\langle -, - \rangle$ on W and on \tilde{W} respectively; so f and \tilde{f} are G -invariant non-degenerate symmetric bilinear forms on W and \tilde{W} respectively. Let $\alpha : W \rightarrow \tilde{W}$ be an FG -isomorphism. Then α induces a G -invariant non-degenerate symmetric bilinear form f' on W as follows:

$$f'(u, w) := \tilde{f}(\alpha(u), \alpha(w)), \quad \forall u, w \in W.$$

By Lemma 4, there is an FG -automorphism $\beta : W \rightarrow W$ which is compatible with f and f' , i.e.

$$f'(\beta(u), \beta(w)) = f(u, w), \quad \forall u, w \in W.$$

Let $\gamma = \alpha\beta$. Then $\gamma : W \rightarrow \tilde{W}$ is an FG -isomorphism, and for any $u, w \in W$ we have

$$\tilde{f}(\gamma(u), \gamma(w)) = \tilde{f}(\alpha(\beta(u)), \alpha(\beta(w))) = f'(\beta(u), \beta(w)) = f(u, w);$$

that is, γ is an FG -isomorphism compatible with the bilinear forms f and \tilde{f} . Let

$$W' = \{w + \gamma(w) \mid w \in W\} \subseteq W \oplus \tilde{W}.$$

It is a routine to check that W' is a submodule and $W' \cong W$; but, noting that $W \perp \tilde{W}$ and $\text{char } F = 2$, for any $u + \gamma(u) \in W'$ and $w + \gamma(w) \in W'$ with $u, w \in W$ we have

$$\begin{aligned} \langle u + \gamma(u), w + \gamma(w) \rangle &= \langle u, w \rangle + \langle \gamma(u), \gamma(w) \rangle \\ &= f(u, w) + \tilde{f}(\gamma(u), \gamma(w)) \\ &= f(u, w) + f(u, w) = 0. \end{aligned}$$

So $W' \cong W$ is an irreducible FG -submodule of V and $W' \subseteq W'^\perp$, and it is reduced to the Case 1 and (ii) holds by induction again.

Remark. In the proof of Theorem 1, Lemma 4 is quoted only in Case 2 where W and \tilde{W} are self-dual composition factors of V . Thus, as a consequence of the proof, we have the following conclusion.

Proposition 1. *Let G be a finite group of order coprime to the characteristic (not necessary 2) of the finite field F , and V be an FG -module with a G -invariant non-degenerate symmetric bilinear form. If V has no self-dual composition factor, then V has a submodule U such that $U^\perp = U$.*

Now we turn to permutation codes. Let X be a finite set; by $\text{Sym}(X)$ we denote the group of all the permutations of X . If there is a group homomorphism $G \rightarrow \text{Sym}(X)$, then X is called a G -set. In that case, any $g \in G$ is mapped to a permutation: $X \rightarrow X, x \mapsto gx$. Hence, $(gg')x = g(g'x)$ for all $g, g' \in G$ and $x \in X$; and $1x = x$ for all $x \in X$.

Let $FX = \{ \sum_{x \in X} a_x x \mid a_x \in F \}$ be the vector space over F with basis X . Extending the G -action on X linearly, FX becomes an FG -module, called an *FG-permutation module* with permutation basis X , please cf. [1, §12].

We say that C is an *FG-permutation code* of FX , denoted by $C \leq FX$, if C is an FG -submodule of the FG -permutation module FX ; and a permutation code C is said to be *irreducible* if C is an irreducible FG -submodule of FX . Further, if X is a transitive G -set, then any FG -permutation code C of FX is said to be a *transitive permutation code*.

Recall that, for a linear code C of length n over F , a permutation of the components of a word of length n is said to be a *permutation automorphism* of C if the permutation keeps every code word of C still a code word. By $\text{PAut}(C)$ we denote the automorphism group of C consisting of all the permutation automorphisms of C . It is easy to see that C is an FG -permutation code of a G -permutation set X of cardinality n if and only if there is a group homomorphism of G to $\text{PAut}(C)$.

There is a so-called scalar product of any two words of FX as follows:

$$\langle \mathbf{w}, \mathbf{w}' \rangle = \sum_{x \in X} w_x w'_x, \quad \forall \mathbf{w} = \sum_{x \in X} w_x x, \mathbf{w}' = \sum_{x \in X} w'_x x \in FX,$$

which is obvious a non-degenerate symmetric bilinear form on FX , we call it the *standard inner product* on FX with respect to the permutation basis X . Moreover, the standard inner product is G -invariant, since for any $g \in G$ and any words $\mathbf{w} = \sum_{x \in X} w_x x$ and $\mathbf{w}' = \sum_{x \in X} w'_x x$ of FX , we have

$$\begin{aligned} \langle g(\mathbf{w}), g(\mathbf{w}') \rangle &= \left\langle g\left(\sum_{x \in X} w_x x\right), g\left(\sum_{x \in X} w'_x x\right) \right\rangle \\ &= \left\langle \sum_{x \in X} w_x(gx), \sum_{x \in X} w'_x(gx) \right\rangle = \sum_{x \in X} w_x w'_x \\ &= \langle \mathbf{w}, \mathbf{w}' \rangle; \end{aligned}$$

equivalently,

$$\langle g(\mathbf{w}), \mathbf{w}' \rangle = \langle \mathbf{w}, g^{-1}(\mathbf{w}') \rangle, \quad \forall g \in G, \forall \mathbf{w}, \mathbf{w}' \in FX.$$

Thus, FX is a self-dual FG -module. In fact, we can make the duality more precisely. Just like the formula (1), the standard inner product induces an isomorphism

$$FX \xrightarrow{\cong} (FX)^*, \quad \mathbf{u} \longmapsto \mathbf{u}^* := \langle \mathbf{u}, - \rangle,$$

where

$$\mathbf{u}^* : FX \longrightarrow F, \quad \mathbf{w} \longmapsto \mathbf{u}^*(\mathbf{w}) = \langle \mathbf{u}, \mathbf{w} \rangle;$$

and

$$X^* := \{x^* \mid x \in X\}$$

is a G -set with G -action

$$g(x^*) = (g^{-1}x)^*, \quad \forall g \in G, x^* \in X^*,$$

such that $(FX)^*$ is an FG -permutation module of the G -set X^* , and $\mathbf{u} \mapsto \mathbf{u}^*$ is a permutation isomorphism.

Let FX be an FG -permutation module. For any permutation code C of FX , since C is an FG -submodule, $C^\perp = \{\mathbf{w} \in FX \mid \langle \mathbf{c}, \mathbf{w} \rangle = 0, \forall \mathbf{c} \in C\}$ is an FG -submodule again, i.e. C^\perp is a permutation code again. In coding-theoretical notation, C^\perp is said to be the *dual permutation code* of C .

An FG -permutation code $C \leq FX$ is said to be *self-orthogonal* if $C \subseteq C^\perp$. And a permutation code $C \leq FX$ is said to be *self-dual* if $C = C^\perp$.

With the coding-theoretical notation introduced above, from Theorem 1 and Proposition 1, we have the following results at once.

Theorem 2. *Let F be a finite field of characteristic 2, and G be a finite group of odd order, and X be a finite G -set. Then the following are equivalent:*

- (i) *every self-dual composition factor of FX has even multiplicity;*
- (ii) *there is a self-dual FG -permutation code C of FX .*

Proposition 2. *Let G be a finite group of order coprime to the characteristic (not necessary 2) of the field F , and X be a finite G -set. If FX has no self-dual composition factor, then there is a self-dual FG -permutation code of FX .*

3 Self-dual extended transitive permutation codes

If a G -set $X = \{x_0\}$ contains of only one element, then X is said to be the trivial G -set and the permutation module $FX \cong F$ is just the *trivial FG -module*, which is obviously a self-dual module.

An elementary known fact is that, in the semisimple case, for any transitive G -set X the trivial FG -module F is a composition factor of multiplicity 1 of the FG -permutation module FX ; e.g. see [3, Lemma 1]; we denote the unique trivial submodule of FX by F if there is no confusion, thus $FX = F \oplus F^\perp$. By Theorem 1, FX has no self-dual codes.

Let X be a transitive G -set. Let $\hat{X} = X \cup \{x_0\}$ be the disjoint union of X with a trivial G -set $\{x_0\}$, i.e. $x_0 \notin X$. Then $F\hat{X} = FX \oplus Fx_0$, and any permutation code C of $F\hat{X}$ is said to be an *extended transitive permutation code* of FX .

Lemma 5. *Notation as above, and let $n = |X|$. The following are equivalent:*

- (i) *there is a permutation code C of FX such that $C^\perp = C \oplus F$ and, as an element of the field F , $-n$ has a square root in F ;*
- (ii) *there is a self-dual permutation code \hat{C} of $F\hat{X}$.*

Proof. Let $e = \sum_{x \in X} x$; then Fe is the unique submodule of FX which is isomorphic to F , so $Fx_0 \oplus Fe$ is the homogeneous component of $F\hat{X}$ associated with the trivial module F . Noting that $Fx_0 \perp Fe$ and $\langle x_0, x_0 \rangle = 1$ and $\langle e, e \rangle = n \neq 0$ (because $n \mid |G|$ which is coprime to $q = |F|$), we see that $Fx_0 \oplus Fe$ is a non-degenerate submodule of $F\hat{X}$. Thus

$$F\hat{X} = (Fx_0 \oplus Fe) \oplus (Fx_0 \oplus Fe)^\perp$$

and

$$(Fx_0 \oplus Fe)^\perp = (Fx_0)^\perp \cap (Fe)^\perp = FX \cap (Fe)^\perp = \text{Ann}_{FX}(Fe).$$

(ii) \Rightarrow (i). By the formula (3) we have

$$\hat{C} = (\hat{C} \cap (Fx_0 \oplus Fe)) \oplus (\hat{C} \cap \text{Ann}_{FX}(Fe)).$$

From the condition (ii) that $\hat{C}^\perp = \hat{C}$, by Lemma 2(ii), we have

$$\dim(\hat{C} \cap (Fx_0 \oplus Fe)) = 1, \quad \dim(\hat{C} \cap \text{Ann}_{FX}(Fe)) = \frac{n-1}{2}.$$

Set $C = \hat{C} \cap \text{Ann}_{FX}(Fe)$; it is easy to check that, C is a permutation code of FX and $C^\perp = C \oplus Fe$ in FX . On the other hand, for $C \cap (Fx_0 \oplus Fe)$ which is a one-dimensional subspace, we assume that $\lambda \in F$ such that

$$\hat{C} \cap (Fx_0 \oplus Fe) = F \cdot (\lambda x_0 + e);$$

then $\langle \lambda x_0 + e, \lambda x_0 + e \rangle = 0$; i.e.

$$0 = \langle \lambda x_0, \lambda x_0 \rangle + \langle e, e \rangle = \lambda^2 + n;$$

that is, $\lambda^2 = -n$.

(i) \Rightarrow (ii). In FX , since $\dim C + \dim C^\perp = n$, from the condition that $C^\perp = C \oplus Fe$ we have that $\dim C = \frac{n-1}{2}$. Turn to $F\hat{X}$, set $\lambda \in F$ such that $\lambda^2 = -n$ and $\hat{C} := F \cdot (\lambda x_0 + e) \oplus C$; as shown above, the 1-dimensional submodule $F \cdot (\lambda x_0 + e)$ of $Fx_0 \oplus Fe$ is isotropic, hence \hat{C} is an isotropic submodule. But $\dim \hat{C} = \frac{n+1}{2}$; and by Lemma 2, \hat{C} is a self-dual permutation code of $F\hat{X}$.

Remark. In the above lemma, the condition “ $-n$ has a square root in F ” in (i) always satisfies for characteristic 2.

For any positive integer n we denote \mathbb{Z}_n the residue ring of the integer ring \mathbb{Z} modulo n , and denote \mathbb{Z}_n^\times the multiplicity group consisting of all the invertible elements of \mathbb{Z}_n . So q is considered as an element of \mathbb{Z}_n^\times , and we can speak of the order of q in the group \mathbb{Z}_n^\times .

Lemma 6. *Let n be an odd integer coprime to q . The following are equivalent:*

- (i) *The order of q in \mathbb{Z}_n^\times is odd.*
- (ii) *For any prime $p|n$ the order of q in \mathbb{Z}_p^\times is odd.*

Proof. Let $n = p_1^{m_1} \cdots p_k^{m_k}$. By Chinese Remainder Theorem we have the following isomorphism about the multiplicative groups:

$$\mathbb{Z}_n^\times \xrightarrow{\cong} \mathbb{Z}_{p_1^{m_1}}^\times \times \cdots \times \mathbb{Z}_{p_k^{m_k}}^\times, \quad a \mapsto (a, \dots, a)$$

The order of $q \in \mathbb{Z}_n^\times$ is odd if and only if the order $q \in \mathbb{Z}_{p_i^{m_i}}^\times$ is odd for every $i = 1, \dots, k$. Consider the exact sequence of multiplication groups:

$$1 \longrightarrow 1 + p_i \mathbb{Z}_{p_i^{m_i}} \xrightarrow{\text{incl}} \mathbb{Z}_{p_i^{m_i}}^\times \xrightarrow{\rho} \mathbb{Z}_{p_i}^\times \longrightarrow 1$$

where “incl” is the inclusion map and ρ is the natural map:

$$\mathbb{Z}_{p_i}^{\times_{m_i}} \longrightarrow \mathbb{Z}_{p_i}^{\times}, \quad a \longmapsto a.$$

Since the order $|1 + p_i \mathbb{Z}_{p_i}^{m_i}| = p_i^{m_i-1}$ is odd, the order of $q \in \mathbb{Z}_{p_i}^{\times_{m_i}}$ is odd if and only if the order of $q \in \mathbb{Z}_{p_i}^{\times}$ is odd.

Recall that F is a finite field of order q . For any positive integer n , in a suitable extension we can take a primitive n 'th root ξ_n of unity, and the extension $F(\xi_n)$ is independent of the choice of ξ_n ; and the order of the Galois group $|\text{Gal}(F(\xi_n)/F)| = |F(\xi_n) : F|$ is just the order of q in the multiplicative group \mathbb{Z}_n^{\times} . As a consequence we have the following at once.

Corollary 1. *Let n be an odd integer coprime to q . The following are equivalent:*

- (i). *The extension degree $|F(\xi_n) : F|$ is odd.*
- (ii). *For any prime $p|n$ the extension degree $|F(\xi_p) : F|$ is odd.*

Let H be a subgroup of the group G , and let Y be a finite H -set; then FY is an FH -permutation module. We have the induced FG -module

$$\text{Ind}_H^G(FY) = FG \bigotimes_{FH} FY = \bigoplus_{t \in T} t \otimes FY,$$

where T is a representative set of the left cosets of G over H ; and $\text{Ind}_H^G(FY)$ is a vector space with basis

$$X := \text{Ind}_H^G(Y) = \bigcup_{t \in T} t \otimes Y = \bigcup_{t \in T} \{t \otimes y \mid y \in Y\}$$

which is a G -set with G -action as follows:

$$g(t \otimes y) = t_g \otimes t_g^{-1} g t y, \quad \forall \quad g \in G, \quad t \in T, \quad y \in Y,$$

where t_g is the representative of the unique left coset $t_g H$ such that $gt \in t_g H$, or equivalently $t_g^{-1} g t \in H$. We say that $\text{Ind}_H^G(FY)$ is the *induced FG -permutation module* with the *induced G -set* $\text{Ind}_H^G(Y)$.

Lemma 7. *Notation as above; and let D be an FH -permutation code of the FH -permutation module FY ; then*

$$\text{Ind}_H^G(D)^\perp = \text{Ind}_H^G(D^\perp).$$

Proof. It is obvious that the induced module $C := \text{Ind}_H^G(D)$ is a submodule of $\text{Ind}_H^G(FY) = \bigoplus_{t \in T} t \otimes FY$, and we have a direct decomposition of F -spaces:

$$\text{Ind}_H^G(D) = \bigoplus_{t \in T} t \otimes D,$$

where each $t \otimes D$ is an F -subspace of $t \otimes FY$. Each $t \otimes FY$ is an F -space with bases $t \otimes Y$, hence with the standard inner product:

$$\left\langle \sum_{y \in Y} a_y(t \otimes y), \sum_{y \in Y} b_y(t \otimes y) \right\rangle = \sum_{y \in Y} a_y b_y;$$

and

$$FY \longrightarrow t \otimes FY, \quad \sum_{y \in Y} a_y y \longmapsto \sum_{y \in Y} a_y (t \otimes y),$$

is an isometric F -isomorphism. With respect to the isometries, it is clear that $(t \otimes D)^\perp = t \otimes D^\perp$; hence

$$\text{Ind}_H^G(D)^\perp = \bigoplus_{t \in T} (t \otimes D)^\perp = \bigoplus_{t \in T} t \otimes D^\perp = \text{Ind}_H^G(D^\perp).$$

Lemma 8. *Let p be an odd prime which is coprime to q such that the order of q in \mathbb{Z}_p^\times is odd. Let A be a finite abelian p -group, and H be a finite group of odd order which acts on the group A . Then there is a group code $C \leq FA$ which is stable by the action of H and $C^\perp = C \oplus F$, where F denotes the unique trivial module of FA .*

Proof. Let $|A| = n$ which is a power of p ; take a primitive n 'th root ξ of unity, and denote $\tilde{F} = F(\xi)$. Then $\tilde{F}A$ is a splitting semisimple commutative algebra. Let $\Gamma = \text{Gal}(\tilde{F}/F)$ denote the Galois group of $\tilde{F} = F(\xi)$ over F ; by Lemma 6 and its corollary, $|\Gamma|$ is odd.

Let A^* denote the set of all the irreducible characters of A over \tilde{F} (i.e. all the homomorphisms $\chi : A \rightarrow \tilde{F}^\times$). With the usual multiplication of functions, A^* is an abelian group and $A^* \cong A$. Note that for any integer k ,

$$\chi^k(a) = \chi(a^k), \quad \forall \chi \in A^*, a \in A.$$

in particular, $\chi^{-1}(a) = \chi(a^{-1})$.

Each $\chi \in A^*$ corresponds exactly one irreducible module $\tilde{F}e_\chi$ of $\tilde{F}A$, where

$$e_\chi = \frac{1}{n} \sum_{a \in A} \chi(a^{-1})a$$

is a primitive idempotent of the algebra $\tilde{F}A$. And we have the direct decomposition of irreducible $\tilde{F}A$ -modules:

$$\tilde{F}A = \bigoplus_{\chi \in A^*} \tilde{F}e_\chi.$$

For $\chi, \psi \in A^*$ and $\lambda, \mu \in \tilde{F}$, the standard inner product

$$\langle \lambda e_\chi, \mu e_\psi \rangle = n\lambda\mu \cdot (\chi|\psi^{-1}),$$

where $(\chi|\psi^{-1})$ denotes the usual inner product of characters:

$$(\chi|\psi^{-1}) = \frac{1}{n} \sum_{a \in A} \chi(a)\psi^{-1}(a^{-1}) = \frac{1}{n} \sum_{a \in A} \chi(a)\psi(a).$$

By the orthogonal relations of characters,

$$\langle \tilde{F}e_\chi, \tilde{F}e_\psi \rangle = \begin{cases} \tilde{F}, & \text{if } \chi = \psi^{-1}, \\ 0, & \text{otherwise.} \end{cases}$$

Any submodule \tilde{C} of $\tilde{F}A$ corresponds exactly to a subset $B \subseteq A^*$ such that

$$\tilde{C} = \bigoplus_{\chi \in B} \tilde{F}e_\chi.$$

Thus

$$\tilde{C}^\perp = \bigoplus_{\psi \notin B^{-1}} \tilde{F}e_\psi$$

where $B^{-1} := \{\chi^{-1} \mid \chi \in B\}$; in particular, \tilde{C} is self-orthogonal code if and only if $B \cap B^{-1} = \emptyset$.

Recall that $\Gamma = \text{Gal}(\tilde{F}/F)$ is a cyclic group generated by the following automorphism

$$\gamma: F(\xi) \longrightarrow F(\xi), \quad \lambda \longmapsto \lambda^q.$$

The group Γ acts on \tilde{F} hence acts on the ring $\tilde{F}A$ in the following way:

$$\gamma\left(\sum_{a \in A} \lambda_a a\right) = \sum_{a \in A} \gamma(\lambda_a) a, \quad \forall \sum_{a \in A} \lambda_a a \in \tilde{F}A.$$

We denote $(\tilde{F}A)^\Gamma$ the subring consisting of all the Γ -fixed elements of $\tilde{F}A$. It is obvious that $(\tilde{F}A)^\Gamma = FA$.

And Γ acts on the set $\{e_\chi \mid \chi \in A^*\}$ of the primitive idempotents of $\tilde{F}A$:

$$\gamma(e_\chi) = \gamma\left(\frac{1}{n} \sum_{a \in A} \chi(a^{-1}) a\right) = \frac{1}{n} \sum_{a \in A} \gamma(\chi(a^{-1})) a = e_{\gamma(\chi)},$$

where $\gamma(\chi) \in A^*$ is the composition homomorphism

$$A \xrightarrow{\chi} \tilde{F} \xrightarrow{\gamma} \tilde{F}, \quad a \longmapsto \gamma(\chi(a)) = (\chi(a))^q,$$

i.e. $\gamma(\chi) = \chi^q$. In this way, Γ acts on the abelian group A^* .

On the other hand, H acts on the ring $\tilde{F}A$:

$$h\left(\sum_{a \in A} \lambda_a a\right) = \sum_{a \in A} \lambda_a h(a), \quad \forall \sum_{a \in A} \lambda_a a \in \tilde{F}A.$$

Similarly, H acts on the set $\{e_\chi \mid \chi \in A^*\}$ of the primitive idempotents of $\tilde{F}A$:

$$h(e_\chi) = h\left(\frac{1}{n} \sum_{a \in A} \chi(a^{-1}) a\right) = \frac{1}{n} \sum_{a \in A} \chi(a^{-1}) h(a) = \frac{1}{n} \sum_{b \in A} \chi(h^{-1}(b^{-1})) b = e_{h(\chi)},$$

where $h(\chi) \in A^*$ is the composition homomorphism

$$A \xrightarrow{h^{-1}} A \xrightarrow{\chi} \tilde{F}, \quad a \longmapsto \chi(h^{-1}(a)).$$

In this way, H acts on the abelian group A^* .

In a word, $\Gamma \times H$ acts on the ring $\tilde{F}A$, and the action induces the action of $\Gamma \times H$ on the abelian group A^* .

Let $C \leq FA$ be an H -stable submodule; denote $\tilde{C} = \tilde{F} \otimes_F C$. Then \tilde{C} is a both H -stable and Γ -stable submodule of $\tilde{F}A$ such that $\tilde{C}^\Gamma = C$. Let $B \subset A^*$

be the subset such that $\tilde{C} = \bigoplus_{\chi \in B} \tilde{F}e_\chi$. Since \tilde{C} is H -stable, we see that B is H -stable; and similarly, B is Γ -stable. So B is a $(\Gamma \times H)$ -stable subset of A^* .

Conversely, if B is a $(\Gamma \times H)$ -stable subset of A^* , then $\tilde{C} = \bigoplus_{\chi \in B} \tilde{F}e_\chi$ is a $(\Gamma \times H)$ -stable submodule of $\tilde{F}A$, and \tilde{C}^Γ is an H -stable submodule of FA .

Let Ω be a non-trivial $(\Gamma \times H)$ -orbit of A^* , i.e. $1 \notin \Omega$. Let $\chi \in \Omega$, then $\chi \neq 1$ hence the order of χ is a power of p , say p^ℓ (recall that $A^* \cong A$ is an abelian p -group). We claim that $\chi^{-1} \notin \Omega$. Suppose it is not the cases, then there is $\gamma^i \in \Gamma$ and $h \in H$ such that $\gamma^i h(\chi) = \chi^{-1}$, and

$$h(\chi) = \gamma^{-i}(\chi^{-1}) = \chi^{(-1)(-q^i)} = \chi^{q^i};$$

thus $\langle \gamma \rangle \times \langle h \rangle$ acts on the cyclic group $\langle \chi \rangle$ of order p^ℓ , and $\gamma^i h$ acts on $\langle \chi \rangle$ as the involution $\chi \mapsto \chi^{-1}$; but the automorphism group $\text{Aut}(\langle \chi \rangle)$ is a cyclic group, hence the product $\gamma^i h$ of the two automorphisms γ^i and h of odd order still has odd order; it contradicts to that the $\chi \mapsto \chi^{-1}$ is an involution.

The involution $\tau : A^* \rightarrow A^*$, $\chi \mapsto \chi^{-1}$, commutes with both Γ and H clearly. So τ permutes all the $(\Gamma \times H)$ -orbits of A^* . For any non-trivial orbit $\Omega \neq \{1\}$, since $\tau(\chi) \notin \Omega$ for any $\chi \in \Omega$, the subset $\tau(\Omega)$ is an orbit different from Ω . Thus we can partition all the non-trivial orbits into two collections B and $B^{-1} = \{\chi^{-1} \mid \chi \in B\}$, and we get the disjoint union

$$A^* = \{1\} \cup B \cup B^{-1}.$$

Then the code $\tilde{C} = \bigoplus_{\chi \in B} \tilde{F}e_\chi$ is H -stable and $\tilde{C}^\perp = \tilde{C} \oplus \tilde{F}$; hence the code $C = \tilde{C}^\Gamma$ of FA is H -stable and $C^\perp = C \oplus F$.

Theorem 3. *Let G be a finite group of odd order, and X be a finite transitive G -set and $n = |X|$. Assume that $q = |F|$ is coprime to n , and the order of q in the multiplicative group \mathbb{Z}_n^\times is odd. Then there is a permutation code $C \leq FX$ such that $C^\perp = C \oplus F$.*

Proof. We prove it by induction on the order of G . It is trivial for $|G| = 1$. Assume $|G| > 1$. Let $x_1 \in X$ and denote G_1 the stabilizer of x_1 in G . Then G_1 is a subgroup and $FX = \text{Ind}_{G_1}^G(F)$. Since G is solvable by Feit-Thompson Odd Theorem, a minimal normal subgroup A of G is an elementary abelian p -group, where p is a prime. Since A is normal, the product AG_1 is a subgroup of G . There are three cases.

Case 1: $AG_1 = G_1$. Then $A \subseteq G_1$, and hence A is contained in every conjugate of G_1 as A is normal. Thus A acts trivially on X , and X is a G/A -set and FX is a permutation module over G/A . Since $|G/A| < |G|$, the conclusion holds by induction.

Case 2: $AG_1 = G$. Since $A \cap G_1$ is both normal in G_1 and in A , we have that $A \cap G_1$ is normal in $AG_1 = G$; but A is a minimal normal subgroup of G , so $A \cap G_1 = 1$. Then we have a bijection

$$\beta : A \longrightarrow X, \quad a \longmapsto a(x_1).$$

Let A acts on A by left translation, and let G_1 acts on A by conjugation; hence $G = AG_1$ is mapped into the group $\text{Sym}(A)$ of all the permutations of A :

$$(bh)(a) = bhah^{-1}, \quad \forall a, b \in A, h \in H.$$

Noting that G_1 stabilizes x_1 , we have that

$$\beta((bh)(a)) = (bhah^{-1})(x_1) = bha(x_1) = (bh)\beta(a).$$

Thus, mapping $bh \in G$ to the permutation $a \mapsto bhah^{-1}$ of A is an action of G on A , and β is an isomorphism of G -sets. Then $n = |A|$ hence $p|n$, so p is coprime to q , and by the assumption of the lemma, the order of q in \mathbb{Z}_p^\times is odd (see Lemma 6). The conclusion is derived from Lemma 8.

Case 3: $G_1 \not\leq AG_1 \leq G$. In this case,

$$FX \cong \text{Ind}_{G_1}^G(F) = \text{Ind}_{AG_1}^G \text{Ind}_{G_1}^{AG_1}(F).$$

Let $Y = \{gx_1 \mid g \in AG_1\}$, which is an AG_1 -set and $\text{Ind}_{G_1}^{AG_1}(F) \cong FY$. By induction, there is a code $D \leq FY$ such that $D^\perp = D \oplus Fe_Y$ where $e_Y = \sum_{y \in Y} y$. Turn to the permutation module $FX = \text{Ind}_{AG_1}^G(FY)$, by Lemma 7, we have

$$\text{Ind}_{AG_1}^G(D)^\perp = \text{Ind}_{AG_1}^G(D^\perp) = \text{Ind}_{AG_1}^G(D \oplus Fe_Y) = \text{Ind}_{AG_1}^G(D) \oplus \text{Ind}_{AG_1}^G(Fe_Y).$$

Noting that, Fe_Y is the unique trivial module of FY , and

$$\text{Ind}_{AG_1}^G(Fe_Y) = \bigoplus_{t \in G/AG_1} t \otimes Fe_Y;$$

by induction again, there is a code $E \leq \text{Ind}_{AG_1}^G(Fe_Y)$ such that

$$\text{Ann}_{\text{Ind}_{AG_1}^G(Fe_Y)}(E) = E \oplus Fe_X,$$

where $e_X = \sum_{x \in X} x$. So we can write $\text{Ind}_{AG_1}^G(Fe_Y) = E' \oplus E \oplus Fe_X$, and have

$$\text{Ind}_{AG_1}^G(D)^\perp = \text{Ind}_{AG_1}^G(D) \oplus \text{Ind}_{AG_1}^G(Fe_Y) = \text{Ind}_{AG_1}^G(D) \oplus E' \oplus E \oplus Fe_X.$$

Let

$$C = \text{Ind}_{AG_1}^G(D) \oplus E$$

which is a permutation code of FX and

$$\begin{aligned} C^\perp &= \text{Ind}_{AG_1}^G(D)^\perp \cap E^\perp = \text{Ann}_{FX}(\text{Ind}_{AG_1}^G(D)) \cap \text{Ann}_{FX}(E) \\ &= (\text{Ind}_{AG_1}^G(D) \oplus E' \oplus E \oplus Fe_X) \cap \text{Ann}_{\text{Ind}_{AG_1}^G(D) \oplus E' \oplus E \oplus Fe_X}(E) \\ &= (\text{Ind}_{AG_1}^G(D) \oplus E' \oplus E \oplus Fe_X) \cap (\text{Ind}_{AG_1}^G(D) \oplus E \oplus Fe_X) \\ &= \text{Ind}_{AG_1}^G(D) \oplus E \oplus Fe_X \\ &= C \oplus Fe_X. \end{aligned}$$

As a consequence of Theorem and Lemma 5 (cf. its remark), we get the followings at once.

Corollary 2. *Assume that $q = |F|$ is even and $|G|$ is odd and X is a transitive G -set and $n = |X|$. If the order of q in the multiplicity group \mathbb{Z}_n^\times is odd, then there is a self-dual extended code of FX .*

Corollary 3. *Assume that $|G|$ is odd and X is a transitive G -set and $n = |X|$. If $q = |F|$ is coprime to n and the order of q in the multiplicity group \mathbb{Z}_n^\times is odd, and $-n$ has square root in F , then there is a self-dual extended code of FX .*

References

- [1] J. L. Alperin, R. B. Bell, Groups and Representations, GTM 13. Berlin Heidelberg New York: Springer-Verlag, 1995.
- [2] F. Bernhardt, P. Landrock and N. J. A. Sloane, The extended Golay codes considered as ideals, J. Comb. Theory ser.A vol.55, (1990), 235-246.
- [3] Yun Fan, Yuan Yuan, On self-dual permutaiotn codes, Acta Math. Scientia 28B (2008), no.3, 633-638.
- [4] G. Hughes, Structure theorems for group ring codes with an application to self-dual codes, Des, Codes Cryptogr, vol.24(2001), 5-14.
- [5] B. Huppert, Endliche Gruppen I, Berlin Heidelberg New York: Springer-Verlag, 1967.
- [6] B. Huppert, N. Blackburn, Finite Groups II, Berlin Heidelberg New York: Springer-Verlag, 1982.
- [7] C. Martinez-Pérez, W. Williams, Self-dual codes and modules for finite groups in characteristic two, IEEE Trans. Inform. Theory Vol. 50(2004), Issue 8, 1798-1803.
- [8] Graham H. Norton and Ana Salagean, On the Hamming Distance of Linear Codes over a Finite Chain Ring, IEEE Trans. Inform. Theory, vol.46(2000), 1060-1067.
- [9] B.S. Rajan, M.U. Siddiqi, A generalized DFT for abelian codes over \mathbf{Z}_m , IEEE Trans. Inform. Theory vol.40 (1994), 2082-2090.
- [10] J.-P. Serre, Linear Representations of Finite Groups, GTM42, New York, Heidelberg, Berlin, Springer-Verlag, 1977.
- [11] W. Williams, A note on self-dual group codes, IEEE Trans. Inform. Theory vol.48 (2002), 3107-3109.
- [12] J. A. Wood, Duality for modules over finite rings and applications to coding theory, Amer. J. Math. 121(3), 555-575, 1999.